IN THE CLAIMS

1. (Currently Amended) A method for securing updating data from a plurality of apparatuses, each apparatus receiving the updates from a managing center, the updates including patch data accompanied by a control block encrypted by a private asymmetrical key taken from a list of keys included in the managing center, the method comprising the steps of:

(a) selecting by the apparatus of a current public key from a list of public keys stored in a non-volatile memory of the apparatus;

(b) receiving and storing the patch data in a random access memory;

(c) receiving the encrypted control block;

(d) decrypting the encrypted control block using the selected current public key;

(e) verifying that the decrypted control block corresponds to said patch data;

(f) installing the patch data; [[and]]

(g) deactivating the current public key such that a different public key is used to decrypt a next control block; and[[.]]

(h) repeating steps a-g for a subsequent patch data and encrypted control block using a subsequent public key selected by the apparatus from the list of public keys stored in the non-volatile memory, the subsequent public key being different from the current public key deactivated in step (g).

2. (Previously Presented) The method according to Claim 1, wherein the control block includes a signature on the patch data, the signature being a result of a hash function.

3. (Previously Presented) The method according to Claims 1 and 2, wherein the verifying step includes the step of establishing the signature on the received patch and the comparison with the decrypted signature in the control block.

4. (Previously Presented) The method according to Claim 1, wherein the control block includes a symmetrical session key determined by the managing center, the symmetrical session key being used to encrypt the patch data.

5. (Previously Presented) The method according to Claim 1, wherein, for each encrypted control block, a new public key taken from the list is used by the apparatus.

6. (Previously Presented) The method according to Claim 1, wherein the public key is deleted from the list after being used, said key being useless for the next updates.

7. (Previously Presented) The method according to Claim 1, wherein the public keys of the list are used sequentially in a predetermined order during each update.

8. (Previously Presented) The method according to Claim 1, wherein the list of public keys is stored in a non-volatile memory, and wherein a key used for an update is definitively deleted from the memory that authorizes the access to the next key for the subsequent update.

9. (Previously Presented) The method according to Claim 1, wherein, for the updating of the software of an apparatus of an old version to a new version, with a difference between the new version and the old version being greater than one, at least one message encrypted with a private key is added allowing the changing of the current key to the next key in the list, the successful decryption of said message inducing the deactivation of the current key and the selection of the next key.

10. (Previously Presented) The method according to Claim 9, wherein the number of messages corresponds to the number of updates separating the initial version of the apparatus and the final version of the update.

11. (Previously Presented) The method according to Claim 1, wherein an updating installation is followed by an increment on a counter or by moving a pointer indicating the position of the key to be selected from the list during the subsequent update, while the list of keys remains unchanged.

12. (Previously Presented) The method according to Claim 1, wherein the control block is successively encrypted by the keys of the previous updates, each key from the list being used one after the other to decrypt the signature.

13. (Previously Presented) The method according to Claim 1, wherein the apparatuses consist of Pay-TV decoders, an update of a decoder being carried out by downloading, from a managing center, of a patch accompanied by a control block, said block is stored in a Random Access Memory, and is decrypted with a current public key contained in a first non-volatile memory of the decoder, then verified and in the case of correspondence, a command leads the installation of the patch in a second non-volatile memory and the deactivation of the current key.

14. (Previously Presented) The method according to Claim 13, wherein a new list of public keys is transmitted to the decoder, said list replaces the list contained in the first memory containing keys deactivated by previous successful updates.

15. (Currently Amended) A system for securing software updates including patch data, the system comprising:

a processor; and

a non-volatile memory connected to the processor for storing a list of public keys;

wherein the processor is configured to perform the steps of

(a) receiving the patch data;

(b) receiving an encrypted control block associated with the patch data, the encrypted control block being encrypted with an asymmetrical private key selected from a list of keys in a management center;

(c) selecting a public key from the list of public keys stored in the non-volatile memory;

(d) decrypting the encrypted control block using the key selected in the previous step;

(e) verifying that the control block corresponds to the patch data;

(f) installing the patch data if the encrypted control block corresponds to the patch data; and

(g) deactivating the public key used in the decrypting step such that a [[new]] different public key from the list of public keys stored in the non-volatile memory is used to decrypt a subsequent control block; and

(h) repeating steps a-g for a subsequent patch data and encrypted control block using a subsequent public key selected by the apparatus from the list of public keys stored in the non-volatile memory, the subsequent public key being different from the current public key deactivated in step (g).

16. (Previously Presented) The system of claim 15, wherein the memory is an electrically erasable programmable read only memory (EEPROM).

17. (Previously Presented) The system of claim 15, wherein the control block includes a signature on the patch data, the signature being a result of a hash function.

18. (Previously Presented) The system of claim 15, wherein the control block includes a symmetrical session key determined by the managing center, the symmetrical session key being used to encrypt the patch data.